

ON THE DECISION PROBLEMS FOR LINEAR RECURRENCE SEQUENCES

MIN SHA

ABSTRACT. In this paper, we show that for almost all linear recurrence sequences of algebraic numbers with integer coefficients (or rational coefficients), the Skolem Problem is decidable by only testing finitely many terms, whose amount is bounded explicitly by using the initial data. The same is also true for both the Positivity Problem and the Ultimate Positivity Problem of real linear recurrence sequences of algebraic numbers with integer coefficients (or rational coefficients).

1. INTRODUCTION

1.1. Background. Linear recurrence sequences appear almost everywhere in mathematics and computer science, and they have been studied for a very long time; see [11] for a deep and extensive introduction. In this paper, we focus on several decision problems relating to such sequences over the complex numbers \mathbb{C} .

Recall that a linear recurrence sequence of order $m \geq 1$ is a sequence $\{u_n\}_{n=0}^{\infty}$ with elements in \mathbb{C} satisfying a recurrence relation

$$(1.1) \quad u_{n+m} = a_1 u_{n+m-1} + \cdots + a_m u_n \quad (n = 0, 1, 2, \dots),$$

where $a_1, \dots, a_m \in \mathbb{C}$, $a_m \neq 0$ and $u_j \neq 0$ for at least one j in the range $0 \leq j \leq m-1$, and the sequence $\{u_n\}$ does not satisfy a relation of type (1.1) of smaller length.

Here, we call a_1, \dots, a_m the *coefficients* of the sequence $\{u_n\}$, and the *initial data* of $\{u_n\}$ are $a_1, \dots, a_m, u_0, \dots, u_{m-1}$. Moreover, the sequence $\{u_n\}$ is called a linear recurrence sequence of algebraic numbers (resp. integers, rational numbers, real numbers) if all its initial data are algebraic numbers (resp. integers, rational numbers, real numbers).

In the sequel, we abbreviate both ‘linear recurrence sequence’ and ‘linear recurrence sequences’ to ‘LRS’.

2010 *Mathematics Subject Classification.* 11B37, 11C08.

Key words and phrases. Linear recurrence sequence, Skolem Problem, Positivity Problem, Ultimate Positivity Problem.

Several crucial properties of the LRS $\{u_n\}$ rely on its characteristic polynomial, which is defined as

$$(1.2) \quad f(X) = X^m - a_1 X^{m-1} - \cdots - a_m = \prod_{i=1}^k (X - \alpha_i)^{e_i} \in \mathbb{C}[X]$$

with distinct $\alpha_1, \alpha_2, \dots, \alpha_k$ (which are called the *characteristic roots* of $\{u_n\}$) and $e_i > 0$ for $1 \leq i \leq k$. Then, u_n can be expressed as

$$(1.3) \quad u_n = \sum_{i=1}^k f_i(n) \alpha_i^n,$$

where f_i is some polynomial of degree $e_i - 1$ ($i = 1, 2, \dots, k$). We call the sequence $\{u_n\}$ *simple* if $k = m$ (that is $e_1 = \cdots = e_m = 1$) and *non-degenerate* if α_i/α_j is not a root of unity for any $i \neq j$ with $1 \leq i, j \leq k$. If $\{u_n\}$ is non-degenerate, then there are only finitely many integers n such that $u_n = 0$.

For the above LRS $\{u_n\}$, the three decision problems we study are the following:

1. *The Skolem Problem* (SP): does $u_n = 0$ for some n ?
2. *The Positivity Problem* (PP): is $u_n > 0$ for all n ?
3. *The Ultimate Positivity Problem* (UPP): is $u_n > 0$ for all but finitely many n ?

Actually, PP and UPP only make sense for real LRS. Note that SP is widely open in general case.

The above three problems (and related variants) have applications in various areas, such as theoretical biology, software verification, probabilistic model checking, quantum computing, discrete linear dynamical systems, as well as combinatorics, formal languages, etc; see [21] for references. We refer the reader to [20] for a survey on these problems.

There are only few results towards decidability of SP. For such sequences of order 1 and 2, this problem is relatively straightforward. Decidability for LRS of algebraic numbers and of orders 3 and 4 is independently settled positively by Mignotte, Shorey and Tijdeman [18], as well as Vereshchagin [25], while that of order not less than 5 is not known. Decidability of SP is also listed as an open problem and discussed by Tao [24, Section 1.9]; see also [13] for a survey. To taste the difficulty of the problem, we want to point out that Blondel and Portier [4, Corollary 2.1] showed that it is NP-hard to decide whether a given integer LRS has a zero. However, it is known that determining whether a given integer LRS has infinitely many zeros is decidable [3].

Most recently, Ouaknine and Worrell have made breakthroughs on PP and UPP. They have showed that UPP for integer LRS of order 5 or

less is decidable in polynomial time [21], and PP for simple integer LRS of order 9 or less is decidable [22]. Moreover, UPP has been shown to be decidable for simple LRS of rational numbers and of all orders [23] in a non-constructive sense; that is, a given LRS of rational numbers can be certified ultimately positive, but no index threshold is provided beyond which all terms of the sequence are positive. Furthermore, it has been proved that it is NP-hard to decide whether a given integer LRS is non-negative; see [1, Theorem 1].

1.2. Our results. In this paper, we show that the above three problems can be decidable for almost all LRS of algebraic numbers with integer coefficients by testing finitely many initial terms, whose number can be bounded explicitly by a function which is poly-exponential in the initial data. The same is also true for those with rational coefficients; see Theorem 3.5. We also give estimates in some sense on the number of such LRS for which SP might be not decidable explicitly; see Section 3.5.

2. PRELIMINARIES

In this section, we gather some definitions and results which are used later on.

2.1. Basic definitions. Given a polynomial

$$f(X) = a_0X^m + a_1X^{m-1} + \cdots + a_m = a_0(X - \alpha_1) \cdots (X - \alpha_m) \in \mathbb{C}[X]$$

of degree $m \geq 1$, we assume that the roots $\alpha_1, \dots, \alpha_m$ (listed with multiplicities) are labelled so that $|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_m|$. In case $|\alpha_1| = \cdots = |\alpha_k| > |\alpha_{k+1}|$, we say that f has *exactly k roots with maximal modulus*.

In order to interpret the meaning of “almost all” in the results, we introduce the following definition.

Definition 2.1. Given a proposition **P** related to integer polynomials, for integers $m \geq 1$ and $H \geq 1$, we define the sets

$$S_m(H) = \{f(X) = X^m + a_1X^{m-1} + \cdots + a_m \in \mathbb{Z}[X] : \\ |a_i| \leq H, i = 1, \dots, m\}$$

and

$$S_m^*(H) = \{f(X) = a_0X^m + a_1X^{m-1} + \cdots + a_m \in \mathbb{Z}[X] : \\ a_0 \neq 0, |a_i| \leq H, i = 0, 1, \dots, m\}.$$

We say that \mathbf{P} is true for *almost all* monic integer polynomials if for any integer $m \geq 1$ the following limit holds:

$$\lim_{H \rightarrow \infty} \frac{|\{f \in S_m(H) : \mathbf{P} \text{ is true for } f\}|}{|S_m(H)|} = 1.$$

Similarly, \mathbf{P} holds for *almost all* integer polynomials if for any integer $m \geq 1$ the following limit holds:

$$\lim_{H \rightarrow \infty} \frac{|\{f \in S_m^*(H) : \mathbf{P} \text{ is true for } f\}|}{|S_m^*(H)|} = 1.$$

Since the behaviour of a LRS depends heavily on its characteristic polynomial, if a certain property is true for almost all monic integer polynomials (resp. integer polynomials), then we say that the corresponding property is true for *almost all* relevant LRS with integer coefficients (resp. rational coefficients). Note that every LRS with rational coefficients uniquely corresponds to an integer polynomial of content 1.

Definition 2.2. For a polynomial $f(X) \in \mathbb{C}[X]$ of degree greater than 0, it is called *dominant* if it has a simple root whose modulus is strictly greater than the moduli of its remaining roots. If $f(X)$ is dominant, the root with maximal modulus is called the *dominant root* of $f(X)$. The polynomial $f(X)$ is called *non-degenerate* if the quotient of its any two distinct roots is not a root of unity.

The following are two results concerning non-degenerate or dominant integer polynomials: the first result comes from [7, Theorem 1.1] and [8, Theorem 1.1], and the second one is from [7, Theorem 1.4] and [9, Theorem 1.1].

Lemma 2.3. *Almost all monic integer polynomials are non-degenerate and dominant.*

Lemma 2.4. *Almost all integer polynomials are non-degenerate and either have a dominant root, or have exactly two roots with maximal modulus (counted with multiplicity).*

Furthermore, several algorithms given in [8] test whether a given integer polynomial is dominant or not, and they can be easily amended to test whether a given integer polynomial has exactly two roots with maximal modulus.

2.2. Previous results. For SP, Mignotte, Shorey and Tijdeman have proved the following general result; see [18, Corollary 1].

Lemma 2.5. *Let $\{u_n\}$ be a LRS of algebraic numbers defined by (1.1). For its characteristic roots in (1.2), without loss of generality suppose that $|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_k|$. Define an integer r by*

$$|\alpha_1| = |\alpha_2| = \cdots = |\alpha_r| > |\alpha_{r+1}|.$$

If either $r = 1$, or $2 \leq r \leq 3$ and at least one of the numbers α_i/α_j with $1 \leq i < j \leq r$ is not a root of unity, then SP is decidable for $\{u_n\}$.

Combining Lemma 2.5 with Lemma 2.3, it is easy to see that for almost all LRS of algebraic numbers with integer coefficients, SP is decidable; from Lemma 2.4, the same is also true for those with rational coefficients. Now, the remaining problem is to estimate the computational complexity. That is, the goal is to obtain a lower bound for the index n beyond which every term u_n is non-zero.

The following result is a weak form of [2, Theorem 2]; see also [5, Theorem 1] and [12, Theorem 1.3] for the previous results.

Lemma 2.6. *Let $\{u_n\}$ be a real LRS defined by (1.1), and let $f(X)$ be its characteristic polynomial. If f does not have a positive root with maximal modulus, then there are infinitely many integers n such that $u_n > 0$ and also infinitely many integers n such that $u_n < 0$.*

Lemma 2.6 tells us that for PP and UPP, we only need to consider those LRS having a positive characteristic root with maximal modulus.

2.3. Mahler measure and Weil height. Given a polynomial $f(x) = a_0x^m + \cdots + a_m = a_0(x - \alpha_1) \cdots (x - \alpha_m) \in \mathbb{C}[x]$ of degree $m \geq 1$, its *length* is defined by

$$L(f) = |a_0| + \cdots + |a_m|,$$

its *height* by

$$H(f) = \max_{0 \leq i \leq m} |a_i|,$$

and its *Mahler measure* by

$$M(f) = |a_0| \prod_{i=1}^m \max\{1, |\alpha_i|\}.$$

For each $f \in \mathbb{C}[x]$ of degree $m \geq 1$, these quantities are related by the following inequality

$$(2.1) \quad H(f)2^{-m} \leq M(f) \leq H(f)\sqrt{m+1},$$

for instance, see [26, (3.12)]. We also need the so-called Landau's inequality

$$(2.2) \quad M(f) \leq \left(\sum_{i=0}^m |a_i|^2 \right)^{1/2},$$

which was proved, for instance, in [17].

Accordingly, for an algebraic number α , its *Mahler measure* $M(\alpha)$ is defined as the Mahler measure of its minimal polynomial f over the integers \mathbb{Z} , that is, $M(\alpha) = M(f)$.

For a number field K , we denote by M_K the set of all valuations v of K extending the standard infinite and p -adic valuations of the rational numbers \mathbb{Q} : $|2|_v = 2$ if $v \in M_K$ is Archimedean, and $|p|_v = p^{-1}$ if v extends the p -adic valuation of \mathbb{Q} . In particular, if the valuation v of K corresponds to a prime ideal \mathfrak{p} of K lying above a prime number p , we also denote the valuation $| \cdot |_v$ by $| \cdot |_{\mathfrak{p}}$, then for any $\alpha \in K$ we have

$$|\alpha|_{\mathfrak{p}} = p^{-\text{ord}_{\mathfrak{p}}(\alpha)/e_{\mathfrak{p}}},$$

where $\text{ord}_{\mathfrak{p}}(\alpha)$ is the exponent of \mathfrak{p} appearing in the prime decomposition of the fractional ideal $\alpha\mathcal{O}_K$, \mathcal{O}_K is the ring of integers of K , and $e_{\mathfrak{p}}$ is the ramification index of \mathfrak{p} over p . For any $v \in M_K$, let K_v be the completion of K with respect to the valuation v , and let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree of v . When the valuation v corresponds to a prime ideal \mathfrak{p} lying above a prime number p , we also denote K_v by $K_{\mathfrak{p}}$ and \mathbb{Q}_v by $\mathbb{Q}_{\mathfrak{p}}$, respectively.

For the above number field K , the (*Weil*) *absolute logarithmic height* of any non-zero $\alpha \in K$ is defined by

$$(2.3) \quad h(\alpha) = d^{-1} \sum_{v \in M_K} d_v \log \max\{|\alpha|_v, 1\}.$$

Actually, we have

$$(2.4) \quad h(\alpha) = d^{-1} \log M(\alpha),$$

see [26, Lemma 3.10] for a proof.

Given non-zero $\alpha \in K$, in view of (2.3) and $h(\alpha) = h(\alpha^{-1})$, for any valuation $v \in M_K$ we have

$$(2.5) \quad |\log |\alpha|_v| \leq dh(\alpha)/d_v \leq dh(\alpha).$$

In the sequel, we use the following formulas without special reference (see, e.g., [26]). For any $n \in \mathbb{Z}$ and $\beta_1, \dots, \beta_k, \gamma \in \overline{\mathbb{Q}}$, we have

$$\begin{aligned} h(\beta_1 + \dots + \beta_k) &\leq h(\beta_1) + \dots + h(\beta_k) + \log k, \\ h(\beta_1 \dots \beta_k) &\leq h(\beta_1) + \dots + h(\beta_k), \\ h(\gamma^n) &= |n|h(\gamma), \\ h(|\gamma|) &\leq h(\gamma), \\ h(\zeta) &= 0 \quad \text{for any root of unity } \zeta \in \overline{\mathbb{Q}}. \end{aligned}$$

Here, $\overline{\mathbb{Q}}$ stands for the algebraic closure of \mathbb{Q} .

We also need the following result, which is exactly [26, Lemma 3.7].

Lemma 2.7. *Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be a non-zero polynomial in n variables. Then, for any algebraic numbers $\gamma_1, \dots, \gamma_n$, we have*

$$h(f(\gamma_1, \dots, \gamma_n)) \leq \log L(f) + \sum_{i=1}^n h(\gamma_i) \deg_{x_i} f,$$

where $\deg_{x_i} f$ is the partial degree of f related to x_i .

2.4. Separating the moduli of roots. The following lemma is a classical result due to Cauchy; see [19, Corollary 8.3.2].

Lemma 2.8. *Let $f(X) \in \mathbb{C}[X]$ be a polynomial of degree $m \geq 1$ defined by*

$$f(X) = a_0 X^m + a_1 X^{m-1} + \dots + a_m,$$

where $a_0 \neq 0$ and $(a_1, \dots, a_m) \neq (0, \dots, 0)$. Then, for an arbitrary non-zero root x of f , we have

$$\frac{\min_{0 \leq i \leq m} |a_i|}{H(f) + \min_{0 \leq i \leq m} |a_i|} < |x| < 1 + \frac{1}{|a_0|} \max\{|a_1|, \dots, |a_m|\}.$$

We reproduce [8, Lemma 2.4 and Lemma 2.5] as follows.

Lemma 2.9. *Let $f(X) \in \mathbb{Z}[X]$ be a quadratic polynomial. Suppose that f has two real roots α and β with $|\alpha| \neq |\beta|$. Then, we have*

$$||\alpha| - |\beta|| \geq H(f)^{-1}.$$

Lemma 2.10. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $m \geq 2$, and let α and β be two roots of f satisfying $|\alpha| \neq |\beta|$. Then,*

$$(2.6) \quad ||\alpha| - |\beta|| > 2^{m(m-1)/4} (m+1)^{-m^3/4+3m/4-3} H(f)^{-m^3/2+m^2+m/2-2}$$

if both α and β are non-real. If, furthermore, α is real and β is non-real, then

$$(2.7) \quad ||\alpha| - |\beta|| \geq 2^{-m(m-1)(m-2)/2} (m+1)^{-m(m-1)-1/2} H(f)^{-2m(m-1)-1}.$$

Finally, if both α and β are real, then

$$(2.8) \quad ||\alpha| - |\beta|| > (2m+1)^{-3m} H(f)^{2-4m}.$$

Note that for large enough m , (2.8) is better than (2.7), and (2.7) is better than (2.6). However, for small integer m , this might be not true. For simplicity, we put them together into two uniform forms.

Lemma 2.11. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $m \geq 3$, and let α and β be two roots of f satisfying $|\alpha| \neq |\beta|$. Then,*

$$(2.9) \quad ||\alpha| - |\beta|| > 2^{-m(m-1)(m-2)} (m+1)^{-m^3/4+3m/4-6} H(f)^{-m^3+m^2+m/2-2},$$

if furthermore α is real, then

$$(2.10) \quad ||\alpha| - |\beta|| > 2^{-m(m-1)(m-2)/2} (m+1)^{-m(m-1)-6} H(f)^{-2m(m-1)-1}.$$

Proof. Note that (2.6) is automatically contained in (2.9). Since for $m \geq 4$,

$$-m^3/4 + 3m/4 - 6 \leq -m^2 + 3m/4 - 6 < -m^2 + m - 1/2,$$

and for $m \geq 3$,

$$-m^3 + m^2 + m/2 - 2 \leq -2m^2 + m/2 - 2 < -2m^2 + 2m - 1,$$

we can see that (2.7) is implied in (2.9) by considering $m = 3$ individually. In addition, noticing

$$2^{-m(m-1)(m-2)} (m+1)^{-m^3/4+3m/4-6} < 2^{-3m} (m+1)^{-3m} < (2m+1)^{-3m}$$

for $m \geq 4$, we know that (2.8) is included in (2.9).

The inequality (2.10) can be proved similarly by merging (2.7) and (2.8). \square

2.5. Bounding the coefficients. For further deductions, we need to estimate the coefficients in (1.3) when the sequence $\{u_n\}$ is a simple LRS of algebraic numbers.

Lemma 2.12. *Let $\{u_n\}$ be a simple LRS of algebraic numbers of order $m \geq 2$ defined by (1.1), and let $f(X)$ be its characteristic polynomial. Write u_n as*

$$u_n = \sum_{j=1}^m b_j \alpha_j^n,$$

where $\alpha_1, \dots, \alpha_m$ are distinct roots of f and all b_j are non-zero. Then, for any $1 \leq j \leq m$ we have

$$h(b_j) < \sum_{i=0}^{m-1} h(u_i) + 2m \sum_{k \neq j} h(\alpha_k) + m^2 h(\alpha_j) + \frac{3}{2}m^2 - \frac{1}{2}m - 1;$$

furthermore if $f \in \mathbb{Q}[X]$, let δ be the smallest positive integer such that $\delta f(X) \in \mathbb{Z}[X]$, denote $\delta f(X)$ by $f^*(X)$ and write

$$f^*(X) = \sum_{i=0}^m a_i^* X^{m-i} \in \mathbb{Z}[X],$$

then we have

$$(2.11) \quad h(b_j) < \sum_{i=0}^{m-1} h(u_i) + \frac{3}{2}m^2 \log \left(\sum_{i=0}^m |a_i^*|^2 \right) + \frac{3}{2}m^2 - \frac{1}{2}m - 1.$$

Finally, if $f \in \mathbb{Q}[X]$ is irreducible, we have

$$(2.12) \quad h(b_j) < \sum_{i=0}^{m-1} h(u_i) + \frac{3}{2}m \log \left(\sum_{i=0}^m |a_i^*|^2 \right) + \frac{3}{2}m^2 - \frac{1}{2}m - 1.$$

Proof. Here, we follow the arguments in the proof of [10, Theorem 3.1].

Notice that

$$(2.13) \quad (u_0, u_1, \dots, u_{m-1}) = (b_1, b_2, \dots, b_m) \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{m-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \alpha_m & \dots & \alpha_m^{m-1} \end{pmatrix},$$

and $\alpha_1, \dots, \alpha_m$ are distinct. To solve the above system of m linear equations in m unknowns b_1, \dots, b_m , we denote the appearing Vandermonde matrix by $V = (\alpha_i^{j-1})_{1 \leq i, j \leq m}$. By [14, Formula (6)], the inverse of V is given by $V^{-1} = (w_{ij})_{1 \leq i, j \leq m}$, where

$$w_{ij} = \frac{(-1)^{i+j} \sigma_{m-i}(\alpha_1, \dots, \hat{\alpha}_j, \dots, \alpha_m)}{\prod_{n=1}^{j-1} (\alpha_j - \alpha_n) \prod_{k=j+1}^m (\alpha_k - \alpha_j)}$$

and $\sigma_k(\alpha_1, \dots, \hat{\alpha}_j, \dots, \alpha_m)$ stands for the k -th elementary symmetric function in the $m-1$ variables $\alpha_1, \dots, \alpha_m$ without α_j ; for instance, in the case $j = m$, we have $\sigma_1(\alpha_1, \dots, \alpha_{m-1}) = \alpha_1 + \dots + \alpha_{m-1}$ and $\sigma_{m-1}(\alpha_1, \dots, \alpha_{m-1}) = \alpha_1 \cdots \alpha_{m-1}$.

So, for any j with $1 \leq j \leq m$ we have

$$b_j = \sum_{i=1}^m u_{i-1} w_{ij}.$$

Since $\sigma_{m-i}(\alpha_1, \dots, \hat{\alpha}_j, \dots, \alpha_m)$ is a polynomial with coefficients 1 in $m-1$ variables $\alpha_1, \dots, \alpha_m$ (without α_j) of degree $m-i$, length $\binom{m-1}{m-i}$,

and degree 1 in each variable α_k , $k \neq j$, by Lemma 2.7 we find that

$$h(\sigma_{m-i}(\alpha_1, \dots, \hat{\alpha}_j, \dots, \alpha_m)) \leq \log \binom{m-1}{m-i} + \sum_{k \neq j} h(\alpha_k).$$

On the other hand, we observe that

$$\begin{aligned} h\left(\prod_{k \neq j} (\alpha_k - \alpha_j)\right) &\leq \sum_{k \neq j} h(\alpha_k - \alpha_j) \\ &\leq \sum_{k \neq j} (h(\alpha_k) + h(\alpha_j) + \log 2) \\ &= \sum_{k \neq j} h(\alpha_k) + (m-1)h(\alpha_j) + (m-1) \log 2. \end{aligned}$$

Thus, we obtain

$$h(w_{ij}) \leq 2 \sum_{k \neq j} h(\alpha_k) + (m-1)h(\alpha_j) + (m-1) \log 2 + \log \binom{m-1}{m-i}.$$

Hence, for $1 \leq j \leq m$ we conclude that

$$\begin{aligned} h(b_j) &\leq \sum_{i=1}^m (h(u_{i-1}) + h(w_{ij})) + \log m \\ &\leq \sum_{i=0}^{m-1} h(u_i) + 2m \sum_{k \neq j} h(\alpha_k) + m(m-1)h(\alpha_j) \\ &\quad + 2m(m-1) \log 2 + \log m \\ &< \sum_{i=0}^{m-1} h(u_i) + 2m \sum_{k \neq j} h(\alpha_k) + m^2 h(\alpha_j) + \frac{3}{2}m^2 - \frac{1}{2}m - 1, \end{aligned}$$

where we also use the fact that the binomial coefficient $\binom{m-1}{m-i} \leq 2^{m-1}$ for any $1 \leq i \leq m$ and

$$2m(m-1) \log 2 + \log m \leq \frac{3}{2}m^2 - \frac{1}{2}m - 1.$$

This gives the first desired upper bound.

Now we assume that f is a polynomial over \mathbb{Q} . For any $1 \leq i \leq m$, denote by $\deg \alpha_i$ the degree of α_i as an algebraic number, since

$$h(\alpha_i) = \frac{\log M(\alpha_i)}{\deg \alpha_i},$$

we deduce that

$$h(\alpha_i) \leq \log M(\alpha_i) \leq \log M(f^*) \leq \frac{1}{2} \log \left(\sum_{i=0}^m |a_i^*|^2 \right),$$

where the last inequality follows from Landau's inequality (2.2). Then, collecting relevant results yields the inequality (2.11).

Finally, the inequality (2.12) comes from the fact that $\deg \alpha_i = m$ for any $1 \leq i \leq m$ when f is an irreducible polynomial over \mathbb{Q} . \square

In fact, slightly better results can be achieved for such sequences of order 2.

Lemma 2.13. *Let $\{u_n\}$ be a simple LRS of algebraic numbers defined by (1.1) of order 2. Let $f(X)$ and $f^*(X)$ be defined as in Lemma 2.12, and write u_n as*

$$u_n = b_1 \alpha_1^n + b_2 \alpha_2^n,$$

where α_1, α_2 are roots of f . Then, we have

$$h(b_j) \leq h(u_0) + h(u_1) + \frac{3}{2} \log \left(\sum_{i=0}^2 |a_i^*|^2 \right) + \frac{3}{2}$$

for $j = 1, 2$.

Proof. Since for $n \geq 0$

$$u_n = b_1 \alpha_1^n + b_2 \alpha_2^n,$$

we derive

$$b_1 = \frac{u_1 - u_0 \alpha_2}{\alpha_1 - \alpha_2} \quad \text{and} \quad b_2 = \frac{u_0 \alpha_1 - u_1}{\alpha_1 - \alpha_2}.$$

So, we obtain

$$\begin{aligned} h(b_1) &\leq h(u_1 - u_0 \alpha_2) + h(\alpha_1 - \alpha_2) \\ &\leq h(u_0) + h(u_1) + h(\alpha_1) + 2h(\alpha_2) + 2 \log 2 \\ &< h(u_0) + h(u_1) + \frac{3}{2} \log \left(\sum_{i=0}^2 |a_i^*|^2 \right) + \frac{3}{2}. \end{aligned}$$

Similarly, we have

$$h(b_2) < h(u_0) + h(u_1) + \frac{3}{2} \log \left(\sum_{i=0}^2 |a_i^*|^2 \right) + \frac{3}{2}.$$

\square

2.6. Linear form in the logarithms of algebraic numbers. One key technical tool in this paper is Baker's inequality on linear form in the logarithms of algebraic numbers. Here we restate one of its explicit forms due to Matveev [16, Corollary 2.3].

First, recall that for a non-zero complex number z , the principal value of the natural logarithm of z is

$$\log z = \log |z| + \sqrt{-1} \cdot \text{Arg } z,$$

where $\text{Arg } z$ is the principal value of the argument of z ($-\pi < \text{Arg } z \leq \pi$). Note that the definition here coincides with the natural logarithm of positive real numbers. We also want to indicate that the identity $\log(z_1 z_2) = \log z_1 + \log z_2$ can fail in our settings.

Let

$$\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_k \log \alpha_k,$$

where $k \geq 2$, $b_1, \dots, b_k \in \mathbb{Z}$, and $\alpha_1, \dots, \alpha_k$ are non-zero elements of a number field K . Let $D = [K : \mathbb{Q}]$ and $B = \max\{|b_1|, \dots, |b_k|\}$. For any $1 \leq j \leq k$, choose real number A_j such that

$$A_j \geq \max\{Dh(\alpha_j), |\log \alpha_j|\}.$$

Suppose that $\Lambda \neq 0$. Then, we have

$$(2.14) \quad \log |\Lambda| > -2^{6k+20} D^2 A_1 \cdots A_k \log(eD) \log(eB),$$

where e is the base of the natural logarithm.

3. MAIN RESULTS

3.1. Characteristic polynomials with dominant roots. We first want to get explicit versions of some results in Lemma 2.5 in Section 3.1 and in Section 3.2.

Theorem 3.1. *Let $\{u_n\}$ be a real simple LRS of algebraic numbers defined by (1.1) of order $m \geq 3$, and let $f(X)$ be its characteristic polynomial. Suppose that $f(X)$ is a polynomial over \mathbb{Q} and has a dominant root, and denote by d the degree of the number field generated by u_0, \dots, u_{m-1} over \mathbb{Q} . Let δ be the smallest positive integer such that $\delta f(X) \in \mathbb{Z}[X]$. Denote $\delta f(X)$ by $f^*(X)$, and write*

$$f^*(X) = \sum_{i=0}^m a_i^* X^{m-i} \in \mathbb{Z}[X].$$

Then, for the sequence $\{u_n\}$, SP, PP and UPP are all decidable by only testing the first $\lfloor N_1(u) \rfloor$ terms, where

$$N_1(u) = 2^{m(m-1)(m-2)/2} (m+1)^{m(m-1)+6} H(f^*)^{2m(m-1)+2} C_1(u)$$

and

$$C_1(u) = m! \cdot 4d \left(\sum_{i=0}^{m-1} h(u_i) + \frac{3}{2}m^2 \log\left(\sum_{i=0}^m |a_i^*|^2\right) + \frac{3}{2}m^2 - \frac{1}{2}m \right);$$

if furthermore $f(X)$ is irreducible, then $C_1(u)$ can be replaced by

$$C_2(u) = m! \cdot 4d \left(\sum_{i=0}^{m-1} h(u_i) + \frac{3}{2}m \log\left(\sum_{i=0}^m |a_i^*|^2\right) + \frac{3}{2}m^2 - \frac{1}{2}m \right).$$

Finally, if $f(X)$ is an irreducible polynomial over \mathbb{Q} having only real roots, then we can choose

$$N_1(u) = (2m+1)^{3m} H(f^*)^{4m-1} C_2(u).$$

Proof. Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be the roots of f^* such that $|\alpha_1| > |\alpha_j|$ for any $2 \leq j \leq m$. Note that they are all distinct and also the roots of f . We also note that α_1 is a real number.

Denote

$$r(u) = 2^{-m(m-1)(m-2)/2} (m+1)^{-m(m-1)-6} H(f^*)^{-2m(m-1)-1}.$$

Then, by (2.10) for any $2 \leq j \leq m$ we have

$$(3.1) \quad |\alpha_1| - |\alpha_j| > r(u).$$

As mentioned before, for any integer $n \geq 0$, u_n can be expressed as

$$u_n = \sum_{j=1}^m b_j \alpha_j^n,$$

where b_1, \dots, b_m are all non-zero complex numbers. Under the assumptions, we know

$$\lim_{n \rightarrow \infty} \frac{u_n}{\alpha_1^n} = b_1.$$

Since the sequence $\{u_n/\alpha_1^n\}$ is a real sequence, b_1 must be a real number.

Now, we want to find a lower bound for n such that

$$(3.2) \quad |b_1 \alpha_1^n| > \sum_{j=2}^m |b_j \alpha_j^n|.$$

So, the sign of u_n is the same as that of $b_1 \alpha_1^n$ when the index n is greater than this lower bound. Then, everything is done. Note that it is equivalent to require that

$$|b_1| > \sum_{j=2}^m |b_j| (|\alpha_j|/|\alpha_1|)^n,$$

which, by (3.1), follows from the inequality

$$(3.3) \quad |b_1| > \sum_{j=2}^m |b_j| (1 - r(u)/|\alpha_1|)^n.$$

On the other hand, for any $1 \leq j \leq m$, by (2.5) we know that

$$|\log |b_j|| \leq [\mathbb{Q}(b_j) : \mathbb{Q}] h(b_j).$$

Since $b_j \in \mathbb{Q}(u_0, \dots, u_{m-1}, \alpha_1, \dots, \alpha_m)$ by (2.13) and $[\mathbb{Q}(\alpha_1, \dots, \alpha_m) : \mathbb{Q}] \leq m!$ ($m!$ is the factorial of m), we have $[\mathbb{Q}(b_j) : \mathbb{Q}] \leq m! \cdot d$. So

$$|\log |b_j|| \leq m! \cdot d h(b_j).$$

Using (2.11), we get

$$|\log |b_j|| \leq B(u),$$

that is

$$(3.4) \quad \exp(-B(u)) \leq |b_j| \leq \exp(B(u))$$

for any $1 \leq j \leq m$, where

$$(3.5) \quad B(u) = m! \cdot d \left(\sum_{i=0}^{m-1} h(u_i) + \frac{3}{2} m^2 \log \left(\sum_{i=0}^m |a_i^*|^2 \right) + \frac{3}{2} m^2 - \frac{1}{2} m - 1 \right).$$

Thus, the inequality (3.3) is implied in the following inequality

$$\exp(-B(u)) > m \exp(B(u)) (1 - r(u)/|\alpha_1|)^n,$$

which is equivalent to

$$n > \frac{2B(u) + \log m}{-\log(1 - r(u)/|\alpha_1|)}.$$

By Lemma 2.8, it suffices to ensure that

$$n > \frac{2B(u) + \log m}{-\log(1 - r(u)/(1 + H(f^*)))}.$$

Using the Taylor expansion $-\log(1 - z) = z + z^2/2 + z^3/3 + \dots$ for $|z| < 1$, it suffices to require that

$$(3.6) \quad n > \frac{2B(u) + \log m}{r(u)/(1 + H(f^*))}.$$

Thus, we get the following lower bound implying the inequality (3.2)

$$(3.7) \quad n > 2^{m(m-1)(m-2)/2} (m+1)^{m(m-1)+6} H(f^*)^{2m(m-1)+2} C_1(u).$$

So, if integer n satisfies the inequality (3.7), then the sign of u_n is the same as that of $b_1 \alpha_1^n$, especially $u_n \neq 0$. This completes the proof of the first desired result.

When f is an irreducible polynomial over \mathbb{Q} , one can prove the remaining desired results by applying the same arguments and using (2.8) and (2.12). \square

From the above proof it is easy to see that only with respect to SP, Theorem 3.1 is also true for non-real simple LRS of algebraic numbers. This also holds for Theorems 3.2 and 3.3.

3.2. Characteristic polynomials with exactly two roots of maximal modulus. The case when the sequence $\{u_n\}$ has exactly two characteristic roots with maximal modulus is quite different from the above case and is more complicated.

Theorem 3.2. *Let $\{u_n\}$, $f(X)$, $f^*(X)$, d be defined as in Theorem 3.1. Suppose that f has exactly two roots, say α_1 and α_2 , with maximal modulus such that α_1/α_2 is not a root of unity. Then, for the sequence $\{u_n\}$, SP is decidable by only testing the first $\lfloor N_2(u) \rfloor$ terms, where*

$$N_2(u) = 2C_3(u) \log C_3(u)$$

and

$$C_3(u) = F(m, d) H(f^*)^{m^3 - m^2 - m/2 + 3.5} C_1(u),$$

$$F(m, d) = 2^{m(m-1)(m-2)+42} \pi(m! \cdot d)^{3.5} (m+1)^{m^3/4 - 3m/4 + 6.5},$$

if furthermore $f(X)$ is irreducible, then $C_1(u)$ can be replaced by $C_2(u)$. Here, $C_1(u)$ and $C_2(u)$ have been defined in Theorem 3.1.

Proof. Under the assumptions, we write $f(X)$ as

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m) \in \mathbb{Q}[X]$$

such that $\alpha_1, \alpha_2, \dots, \alpha_m$ are all distinct and $|\alpha_1| = |\alpha_2| > |\alpha_j|$ for any $3 \leq j \leq m$. By (2.9), for any $3 \leq j \leq m$ we have

$$|\alpha_1| - |\alpha_j| > s(u),$$

where

$$s(u) = 2^{-m(m-1)(m-2)} (m+1)^{-m^3/4 + 3m/4 - 6} H(f^*)^{-m^3 + m^2 + m/2 - 2}.$$

Note that for any integer $n \geq 0$, u_n can be expressed as

$$u_n = \sum_{j=1}^m b_j \alpha_j^n,$$

where b_1, \dots, b_m are all non-zero complex numbers.

In the sequel, we want to find a lower bound for n such that

$$(3.8) \quad |b_1 \alpha_1^n + b_2 \alpha_2^n| > \sum_{j=2}^m |b_j \alpha_j^n|.$$

So, whenever the index n is greater than this lower bound, we have $u_n \neq 0$. This can complete the proof.

The key step is to get a lower bound for the left-hand side of (3.8) by using Baker's inequality on linear form (2.14). Then, let the right-hand side of (3.8) be less than the lower bound, this can give the desired lower bound for the index n .

For $n \geq 0$, we have

$$(3.9) \quad |b_1\alpha_1^n + b_2\alpha_2^n| = |b_1\alpha_1^n| \cdot \left| (-1) \cdot \frac{b_2}{b_1} \cdot \left(\frac{\alpha_2}{\alpha_1}\right)^n - 1 \right|$$

Here, for $n \geq 0$ we put

$$\Delta_n = (-1) \cdot \frac{b_2}{b_1} \cdot \left(\frac{\alpha_2}{\alpha_1}\right)^n - 1,$$

and

$$(3.10) \quad \Lambda_n = \log(\Delta_n + 1).$$

Then, by definition, there exists an odd integer a such that $|a| \leq n+1$ and

$$\Lambda_n = a \log(-1) + \log(b_2/b_1) + n \log(\alpha_2/\alpha_1),$$

which gives a linear form in the logarithms of algebraic numbers. We need to handle the exceptional case when $\Lambda_n = 0$.

In the following, we assume that

$$(3.11) \quad |\Delta_n| \leq 1/2.$$

If this is not true, then later on one can see that this implies much better results; see (3.12) and (3.19).

Notice that for any complex number z with $0 < |z| \leq r < 1$, using the Taylor expansion, we have

$$\begin{aligned} |\log(1+z)| &= \left| z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots \right| \\ &\leq \left| 1 + \frac{r}{2} + \frac{r^2}{3} + \cdots \right| \cdot |z| = \frac{|\log(1-r)|}{r} |z|. \end{aligned}$$

Using this estimate together with (3.10) and (3.11), we obtain

$$(3.12) \quad \frac{1}{2} |\Lambda_n| = \frac{1}{2} |\log(\Delta_n + 1)| < |\Delta_n|.$$

Suppose that $\Lambda_n = 0$. Then $\Delta_n = 0$, that is $b_1\alpha_1^n + b_2\alpha_2^n = 0$. Let

$$K = \mathbb{Q}(u_0, \dots, u_{m-1}, \alpha_1, \dots, \alpha_m).$$

Then, $[K : \mathbb{Q}] \leq m! \cdot d$. If α_1/α_2 is not a unit of K , then there exists a prime ideal \mathfrak{p} in the ring of integers of K such that $\text{ord}_{\mathfrak{p}}(\alpha_1/\alpha_2)$ is non-zero. Then, we get

$$(3.13) \quad n \leq n|\text{ord}_{\mathfrak{p}}(\alpha_1/\alpha_2)| = |\text{ord}_{\mathfrak{p}}(b_2/b_1)| \leq |\text{ord}_{\mathfrak{p}}(b_1)| + |\text{ord}_{\mathfrak{p}}(b_2)|.$$

On the other hand, by definition, for any $1 \leq j \leq m$, we know that

$$|b_j|_{\mathfrak{p}} = p^{-\text{ord}_{\mathfrak{p}}(b_j)/e_{\mathfrak{p}}},$$

where p is the underlying prime number of \mathfrak{p} , and $e_{\mathfrak{p}}$ is the ramification index of \mathfrak{p} over p . Using (2.5), we obtain

$$|\log |b_j|_{\mathfrak{p}}| \leq \frac{[K : \mathbb{Q}]}{d_{\mathfrak{p}}} h(b_j),$$

where $d_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$. Notice that $e_{\mathfrak{p}} \leq d_{\mathfrak{p}}$. So, for any $1 \leq j \leq m$ we have

$$(3.14) \quad |\text{ord}_{\mathfrak{p}}(b_j)| \leq \frac{e_{\mathfrak{p}}[K : \mathbb{Q}]}{d_{\mathfrak{p}} \log p} h(b_j) \leq \frac{[K : \mathbb{Q}]}{\log p} h(b_j) \leq 2B(u),$$

where $B(u)$ has been defined in (3.5). Combining (3.13) with (3.14), we get

$$(3.15) \quad n \leq 4B(u).$$

Now, we suppose that $\Lambda_n = 0$ and α_1/α_2 is a unit of K . Since α_1/α_2 is not a root of unity, there exists an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that $|\sigma(\alpha_1)/\sigma(\alpha_2)| > 1$. By (2.9), we have

$$|\sigma(\alpha_1)| - |\sigma(\alpha_2)| > s(u).$$

Notice that

$$|\sigma(b_2)/\sigma(b_1)| \leq \exp(2B(u)),$$

which can be deduced similarly as (3.4). In view of

$$\sigma(b_1)\sigma(\alpha_1)^n + \sigma(b_2)\sigma(\alpha_2)^n = 0,$$

we deduce that

$$(3.16) \quad |\sigma(\alpha_1)/\sigma(\alpha_2)|^n = |\sigma(b_2)/\sigma(b_1)| \leq \exp(2B(u)).$$

Since

$$|\sigma(\alpha_1)/\sigma(\alpha_2)|^n > (1 + s(u)/|\sigma(\alpha_2)|)^n > (1 + s(u)/(1 + H(f^*)))^n,$$

where the last inequality follows from Lemma 2.8, we consider the inequality

$$(1 + s(u)/(1 + H(f^*)))^n > \exp(2B(u)),$$

which gives

$$n > \frac{2B(u)}{\log(1 + s(u)/(1 + H(f^*)))}.$$

Since $\log(1+z) > z - z^2/2 > z/2$ for $0 < z < 1$, it suffices to require that

$$(3.17) \quad n > \frac{4B(u)(1+H(f^*))}{s(u)}.$$

Notice that the lower bound in (3.17) is much larger than the upper bound in (3.15). Thus, if integer n satisfies (3.17), then the inequality in (3.16) is not true, and we must have $\Lambda_n \neq 0$.

Now, we assume that n satisfies (3.17). So, $\Lambda_n \neq 0$. Applying Baker's inequality (2.14), we find that

$$(3.18) \quad |\Lambda_n| > \exp(-2^{38}D^2A_1A_2A_3\log(eD)\log(en+e)),$$

where D is the degree of the number field generated by b_2/b_1 and α_2/α_1 over \mathbb{Q} , and

$$\begin{aligned} A_1 &= \pi, \\ A_2 &\geq \max\{Dh(b_2/b_1), |\log(b_2/b_1)|\}, \\ A_3 &\geq \max\{Dh(\alpha_2/\alpha_1), |\log(\alpha_2/\alpha_1)|\}. \end{aligned}$$

Since both b_2/b_1 and α_2/α_1 are contained in K , we have

$$D \leq [K : \mathbb{Q}] \leq m! \cdot d.$$

By (2.11), we get

$$Dh(b_2/b_1) \leq D(h(b_1) + h(b_2)) \leq 2B(u).$$

In addition, we note that

$$|\log(b_2/b_1)| \leq \log|b_2/b_1| + \pi \leq Dh(b_2/b_1) + \pi \leq 2B(u) + \pi.$$

Thus, we choose

$$A_2 = \frac{1}{2}C_1(u),$$

where $C_1(u)$ has been defined in Theorem 3.1. It is easy to see that $A_2 > 2B(u) + \pi$.

Now, we want to choose A_3 . Since

$h(\alpha_2/\alpha_1) \leq h(\alpha_2) + h(\alpha_1) \leq 2\log M(f^*) \leq 2\log H(f^*) + \log(m+1)$, where the last inequality follows from (2.1). On the other hand, we have

$$|\log(\alpha_2/\alpha_1)| \leq \log|\alpha_2/\alpha_1| + \pi < 2\log(H(f^*) + 1) + \pi,$$

where the last inequality is derived from Lemma 2.8. So, we can choose

$$A_3 = m! \cdot 2d(m+1)^{0.5}H(f^*)^{0.5}.$$

Define

$$c = 2^{39}D^2A_1A_2A_3\log(eD).$$

Then, under (3.17), the inequality (3.18) becomes

$$(3.19) \quad |\Lambda_n| > \exp(-c \log n),$$

which, together with (3.9) and (3.12), implies that

$$(3.20) \quad |b_1 \alpha_1^n + b_2 \alpha_2^n| > \frac{1}{2} |b_1 \alpha_1^n| \exp(-c \log n).$$

Substituting relevant results into the definition of c , we redefine

$$c = 2^{40} \pi (m! \cdot d)^{3.5} (m+1)^{0.5} H(f^*)^{0.5} C_1(u).$$

Now, we are ready to find a lower bound for n such that

$$|b_1 \alpha_1^n + b_2 \alpha_2^n| > \sum_{j=3}^m |b_j \alpha_j^n|.$$

This is implied in the following inequality by using (3.20)

$$\frac{1}{2} |b_1 \alpha_1^n| \exp(-c \log n) \geq \sum_{j=3}^m |b_j \alpha_j^n|.$$

That is, we need that

$$|b_1| \exp(-c \log n) \geq 2 \sum_{j=3}^m |b_j| (|\alpha_j|/|\alpha_1|)^n,$$

which follows from the inequality

$$(3.21) \quad |b_1| \exp(-c \log n) \geq 2 \sum_{j=3}^m |b_j| (1 - s(u)/|\alpha_1|)^n.$$

By (3.4), the inequality (3.21) is implied in the following inequality

$$\exp(-B(u) - c \log n) \geq 2m \exp(B(u)) (1 - s(u)/|\alpha_1|)^n,$$

which is equivalent to

$$-n \log(1 - s(u)/|\alpha_1|) - c \log n \geq 2B(u) + \log(2m).$$

As in (3.6), it suffices to require that

$$(3.22) \quad ns(u)/(1 + H(f^*)) - c \log n \geq 2B(u) + \log(2m).$$

Notice that the integers n satisfying the following inequalities also satisfies (3.22),

$$(3.23) \quad \begin{cases} c \log n \leq ns(u)/(2 + 2H(f^*)), \\ ns(u)/(2 + 2H(f^*)) \geq 2B(u) + \log(2m). \end{cases}$$

Since the function $x/\log x$ is strictly increasing when $x \geq 3$, for $A \geq 3$, if $x \geq 2A \log A$, then $x/\log x \geq A$. Thus, if

$$(3.24) \quad n \geq 4cs(u)^{-1}(1 + H(f^*)) \log(2cs(u)^{-1}(1 + H(f^*))),$$

then the first inequality in (3.23) holds, and in fact the second one also holds. Note that the lower bound in (3.24) is much bigger than that in (3.17).

Thus, by (3.24) we get the following lower bound for the index n implying the inequality (3.21)

$$(3.25) \quad n > 2C_3(u) \log C_3(u).$$

So, if integer n satisfies the inequality (3.25), then we have

$$|b_1\alpha_1^n + b_2\alpha_2^n| > \sum_{j=3}^m |b_j\alpha_j^n|.$$

Thus, $u_n \neq 0$. This completes the proof of the first desired result.

The remaining desired result follows from (2.12). \square

Following the ideas in [18] and in the proof of Theorem 3.2, one can get an explicit result for Lemma 2.5 in the case when the sequence $\{u_n\}$ is simple and has exactly three roots with maximal modulus. However, this might be very complicated and deserves studying as a separate project.

3.3. Quadratic characteristic polynomials. If the sequence $\{u_n\}$ is of order 2, we can get better results.

Theorem 3.3. *Let $\{u_n\}$ be a real simple LRS of algebraic numbers defined by (1.1) of order 2. Let $f(X), f^*(X), d$ be defined as in Theorem 3.1. If f has a dominant root, then for the sequence $\{u_n\}$, SP, PP and UPP are all decidable by only testing the first $\lfloor N_3(u) \rfloor$ terms, where*

$$N_3(u) = 4dH(f^*)^2 \left(h(u_0) + h(u_1) + \frac{3}{2} \log \left(\sum_{i=0}^2 |a_i^*|^2 \right) + \frac{3}{2} \right).$$

Otherwise if $f(X)$ does not have a dominant root and the quotient of its two roots is not a root of unity, then SP is decidable by only testing the first $\lfloor N_4(u) \rfloor$ terms, where

$$N_4(u) = 8d \left(h(u_0) + h(u_1) + \frac{3}{2} \log \left(\sum_{i=0}^2 |a_i^*|^2 \right) + \frac{3}{2} \right).$$

Proof. Let α_1 and α_2 be the two characteristic roots of $\{u_n\}$. First, we suppose that $|\alpha_1| > |\alpha_2|$. Note that in this case both α_1 and α_2 are real. By Lemma 2.9, we know

$$|\alpha_1| - |\alpha_2| \geq 1/H(f^*).$$

Then, using Lemma 2.13 and applying the same arguments as in the proof of Theorem 3.1, we get that if integer n satisfies

$$n > N_3(u),$$

then the sign of u_n is the same as that of $b_1\alpha_1^n$, especially $u_n \neq 0$. This completes the proof of the first part of the theorem.

Now, we suppose that $|\alpha_1| = |\alpha_2|$. If α_1/α_2 is a unit of K , then in view of $|\alpha_1/\alpha_2| = |\alpha_2/\alpha_1| = 1$, we find that α_1/α_2 is a root of unity, which contradicts the assumption that α_1/α_2 is not a root of unity. So, α_1/α_2 must be not a unit of K . Note that for any integer $n \geq 0$ we have

$$u_n = b_1\alpha_1^n + b_2\alpha_2^n$$

for some non-zero complex numbers b_1 and b_2 , similar as the deductions of (3.15) we conclude that if integer n satisfies

$$n > N_4(u),$$

then $u_n \neq 0$. This completes the proof of the theorem. \square

3.4. Decidability for almost all sequences. As mentioned before, although Theorems 3.1, 3.2 and 3.3 only concern real simple LRS of algebraic numbers, the arguments are still valid for arbitrary simple LRS of algebraic numbers when only considering SP. For example, in this case it is not needed that the coefficient b_1 in the proof of Theorem 3.1 is a real number. We merge them into the following.

Theorem 3.4. *Let $\{u_n\}$ be a simple LRS of algebraic numbers defined by (1.1) of order $m \geq 2$, and let $f(X)$ be its characteristic polynomial. Suppose that f has a dominant root or has exactly two roots with maximal modulus (their quotient is not a root of unity). Then, SP is decidable by only testing finitely many initial terms, whose amount is bounded explicitly by the initial data as in Theorems 3.1, 3.2 or 3.3.*

Now, we are ready to state and prove the key result.

Theorem 3.5. *For almost all LRS of algebraic numbers with integer coefficients (or rational coefficients), SP is decidable by only testing finitely many terms, whose amount is bounded explicitly by the initial data as in Theorems 3.1, 3.2 or 3.3. The same is also true for both PP*

and UPP for real LRS of algebraic numbers with integer coefficients (or rational coefficients).

Proof. Let $\{u_n\}$ be a LRS of algebraic numbers defined by (1.1) of order $m \geq 2$, and let $f(X)$ be its characteristic polynomial.

Suppose that f is an integer polynomial. Note that f is monic. Since almost all monic integer polynomials are irreducible (for example, see [6]), we assume that f is irreducible. Then, $\{u_n\}$ is a simple LRS. By Lemma 2.3, almost all monic integer polynomials have a dominant root. Then, this case of SP is done by applying Theorem 3.4.

Now, assume that f is a polynomial over \mathbb{Q} . Let δ be the smallest positive integer such that $\delta f(X) \in \mathbb{Z}[X]$. δf has the same roots as f , but note that δf may be not monic. Since almost all integer polynomials are irreducible (for example, see [15]), by Lemma 2.4, we only need to consider the case when δf is irreducible and non-degenerate. Furthermore, by Lemma 2.4, we can assume that δf has a dominant root or has exactly two roots with maximal modulus. Then, this case of SP is also established by using Theorem 3.4. Thus, this completes the proof of the first part.

For real LRS of algebraic numbers with integer coefficients (or rational coefficients), the remaining desired results can be proved similarly by using Lemma 2.6 and Theorems 3.1 and 3.3. Note that for an irreducible and non-degenerate characteristic polynomial f , if it has exactly two roots with maximal modulus, then these two root must be non-real, thus this case has been done in Lemma 2.6. \square

3.5. Estimate the exceptional set. Regarding the results in Theorem 3.4, one question of interest is for how many such LRS the Skolem Problem might be not decidable explicitly. It depends on the way how to count LRS.

For LRS of algebraic numbers with integer coefficients of order $m \geq 3$, we define that two LRS are equivalent if they have the same characteristic polynomial. So, it is equivalent to ask for how many such equivalence classes the Skolem Problem might be not decidable explicitly. For the equivalence classes corresponding to the set $S_m(H)$ (defined in Section 2.1), let $A_m(k, H)$ be the number of polynomials $f \in S_m(H)$ having exactly k roots with maximal modulus, then by [9, Theorem 3.2] and [7, Theorem 1.1] we have

$$(3.26) \quad |S_m(H)| - A_m(1, H) - A_m(2, H) \leq c_1(m)H^{m-1},$$

where $c_1(m)$ is a function with respect to m . According to Theorem 3.4, this can be viewed as an answer to the question.

On the other hand, for LRS of algebraic numbers with rational coefficients of order $m \geq 3$, we can define the same equivalent relation. For the equivalence classes corresponding to the set

$$T_m^*(H) = \{f(X)/H : f \in S_m^*(H)\},$$

let $A_m^*(k, H)$ be the number of polynomials $f \in T_m^*(H)$ having exactly k roots with maximal modulus, then by [9, Theorem 3.4] and [7, Theorem 1.4] we have

$$(3.27) \quad |T_m^*(H)| - A_m^*(1, H) - A_m^*(2, H) \leq c_2(m)H^m,$$

where $c_2(m)$ is a function with respect to m . This can be viewed as another answer to the question.

ACKNOWLEDGEMENT

The author want to thank Manas Patra and Igor E. Shparlinski for introducing him into the Skolem Problem and also for useful discussions and helpful comments. The research was supported by the Australian Research Council Grant DP130100237.

REFERENCES

- [1] P.C. Bell, J.-C. Delvenne, R.M. Jungers and V.D. Blondel, *The continuous Skolem-Pisot problem*, Theor. Comput. Sci. **411** (2010), 3625–3634.
- [2] J.P. Bell and S. Gerhold, *On the positivity set of a linear recurrence sequence*, Israel J. Math. **157**(1) (2007), 333–345.
- [3] J. Berstel and M. Mignotte, *Deux propriétés décidables des suites récurrentes linéaires*, Bull. Soc. Math. France **104** (1976), 175–184.
- [4] V.D. Blondel and N. Portier, *The presence of a zero in an integer linear recurrent sequence is NP-hard to decide*, Linear Algebra Appl. **351-352** (2002), 91–98.
- [5] J.R. Burke and W.A. Webb, *Asymptotic behaviour of linear recurrences*, Fibonacci Quart. **19**(4) (1981), 318–321.
- [6] R. Chela, *Reducible polynomials*, J. Lond. Math. Soc. **38** (1963), 183–188.
- [7] A. Dubickas and M. Sha, *Counting degenerate polynomials of fixed degree and bounded height*, Monatsh. Math., DOI 10.1007/s00605-014-0680-9, to appear, <http://arxiv.org/abs/1402.5430>.
- [8] A. Dubickas and M. Sha, *Counting and testing dominant polynomials*, Exper. Math., to appear, <http://arxiv.org/abs/1407.2789>.
- [9] A. Dubickas and M. Sha, *Positive density of integer polynomials with some prescribed properties*, preprint, 2015, <http://arxiv.org/abs/1504.05144>.
- [10] A. Dubickas, M. Sha and I. Shparlinski, *Explicit form of Cassels’ p-adic embedding theorem for number fields*, Can. J. Math., to appear, <http://arxiv.org/abs/1401.6819>.
- [11] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, Am. Math. Soc., Providence, RI, 2003.

- [12] S. Gerhold, *Point lattices and oscillating recurrence sequences*, J. Differ. Equ. Appl. **11**(6) (2005), 515–533.
- [13] V. Halava, T. Harju, M. Hirvensalo and J. Karhumäki, *Skolem’s problem – on the border between decidability and undecidability*, Technical Report 683, Turku Centre for Computer Science, 2005.
- [14] A. Klinger, *The Vandermonde matrix*, Amer. Math. Monthly **74** (1967), 571–574.
- [15] G. Kuba, *On the distribution of reducible polynomials*, Math. Slovaca **59** (2009), 349–356.
- [16] E.M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II*, Izv. Math. **64**(6) (2000), 1217–1269.
- [17] M. Mignotte and P. Glessner, *Landau’s Inequality via Hadamard’s*, J. Symb. Comput. **18**(4) (1994), 379–383.
- [18] M. Mignotte, T.N. Shorey and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math. **349** (1984), 63–76.
- [19] B. Mishra, *Algorithmic algebra*, Springer, New York, 1993.
- [20] J. Ouaknine and J. Worrell, *Decision problems for linear recurrence sequences*, In: Proc. 6th Intern. Workshop on Reachability Problems (RP), LNCS **7550**, pp. 21–28, Springer, 2012.
- [21] J. Ouaknine and J. Worrell, *Positivity problems for low-order linear recurrence sequences*, In: Proc. 25th Symp. on Discrete Algorithms (SODA), pp. 366–379, ACM-SIAM, 2014.
- [22] J. Ouaknine and J. Worrell, *On the Positivity Problem for simple linear recurrence sequences*, In: Proc. 41st Intern. Colloq. on Automata, Languages and Programming (ICALP), LNCS **8573**, pp. 318–329, Springer, 2014.
- [23] J. Ouaknine and J. Worrell, *Ultimate Positivity is decidable for simple linear recurrence sequences*, In: Proc. 41st Intern. Colloq. on Automata, Languages and Programming (ICALP), LNCS **8573**, pp. 330–341, Springer, 2014.
- [24] T. Tao, *Structure and randomness: pages from year one of a mathematical blog*, American Mathematical Society, 2008.
- [25] N.K. Vereshchagin, *Occurrence of zero in a linear recursive sequence*, Math. Notes **38** (1985), 609–615.
- [26] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables*, Grundlehren der Mathematischen Wissenschaften **326**, Springer, Berlin, 2000.

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW 2052, AUSTRALIA
E-mail address: shamin2010@gmail.com